

# NETWORK AND COMPUTER SECURITY

## SUMMARY

Lorenzo De Bie

Academic year: 2020-2021



# CONTENTS

<b>1</b>	<b>Introduction</b>	<b>2</b>
1.1	Security in the media . . . . .	2
1.2	Example Incidents . . . . .	3
1.3	Why do we need security? Why Information Security? . . . . .	3
<b>2</b>	<b>Basic Concepts</b>	<b>4</b>
2.1	A security model . . . . .	4
2.2	Security Goals . . . . .	4
2.2.1	Confidentiality . . . . .	4
2.2.2	Authentication . . . . .	5
2.2.3	Access Control/authorization . . . . .	5
2.2.4	Data integrity . . . . .	6
2.2.5	Non-repudiation . . . . .	7
2.2.6	Availability . . . . .	7
2.3	Security Threats . . . . .	7
2.3.1	Possible attacks . . . . .	8
2.3.2	Categories of attacks . . . . .	8
2.3.3	Desired degree of security? . . . . .	8

# 1 INTRODUCTION

## 1.1 Security in the media

- Security  $\Leftrightarrow$  User friendly: work of security personnel goes unnoticed when everything is good, but they get blamed when things go wrong.
- Users remains a security risk:
  - Due to lack of knowledge: *1 in 10 in a survey think HTML is an STD - Los Angeles Times* [1]
  - Due to incompetence
  - Information can still be shared non-digitally
- Nobody is safe: *NSA hackt Belgische cyberprof - De Standaard* [2]
- Privacy vs Security: sacrificing privacy so data can be used for security.
  - *AIVD hackt internetfora, 'tegen wet in' - NRC* [3]
  - *Révélations sur le Big Brother français* [4]
- Check yourself using <https://haveibeenpwned.com/>
- Privacy vs Health: tracing apps in times of COVID-19
- Journalists aren't always exactly IT experts  $\rightarrow$  remain a critic, remain sceptic
- Future trends: blockchains
  - mainly used for data integrity through **public ledgers**
  - Used to log activity.
    - \* Detect malicious operations, hackers, foreign surveillance, database modifications
    - \* Equally important as access restrictions
- Future trends: cyber warfare
  - Nation wide actions to cause damage or disruption. Can include physical impact and/or harm to human persons
  - Interesting targets: traffic lights, electricity systems, water filtration, power plants
  - Stuxnet:
    - \* Worm that targeted Iranian nuclear facilities, damaging centrifuges and other hardware
    - \* Most likely an American-Israeli cyberweapon
  - Petya: ransomware or state attack?
    - \* Focused strongly on Ukraine systems
    - \* Made very little money
    - \* Either very buggy, or very damaging by purpose: permanent removal of files, nuclear power plants, ministries, metros and banks offline, possible link with assassination of Maksym Shapoval
  - Future trends: IoT: *Docs shielded Cheney defibrillator from hacks - CNN* [5]

## 1.2 Example Incidents

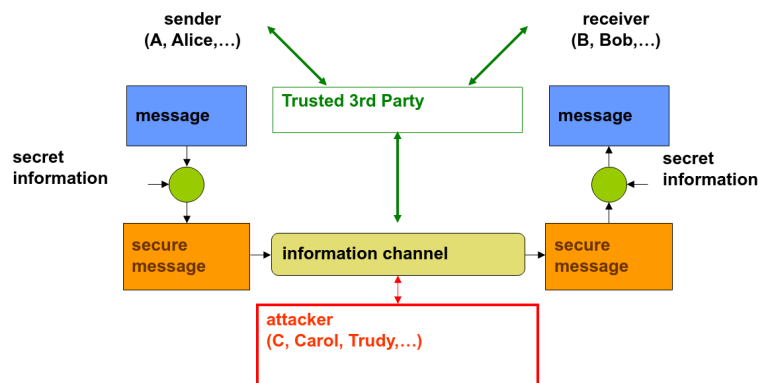
- Ashley Madison (2015)
- DNC email leak (2016)
- Mirai (2016)
- Twitter hack (2020)

## 1.3 Why do we need security? Why Information Security?

- Counterpart of securing material objects
  - Material object have some **value**
  - Can be stolen or damaged
  - Cost for security/protection takes into account value and risk of theft/damage
- Risk of threats against information security is **much** greater
- Value of information sometimes hard to assess, best estimated by damage caused. Losses cannot be undone
- Threats against information include:
  - **Loss** of information
  - **Forged** information
  - **Unauthorised release** of information
  - **Repudiation** of information
- Value of information systems hard to asses. Systems used to enable service →damage when service unavailable or unreliable
- Threats against information systems include:
  - **Unavailability**/disruption of service
  - **Unauthorised acces** to service
  - Threats against exchanged information
- Security measures for information systems:
  - **Information Security**: encryption, virus scanners, firewalls...
  - Carry some cost (installation, maintenance, computation time)
  - dependent on risk and potential damage

## 2 BASIC CONCEPTS

### 2.1 A security model



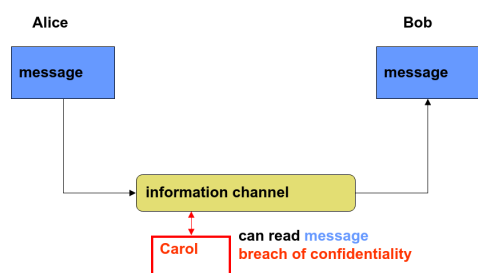
### 2.2 Security Goals

Possible exam questions:

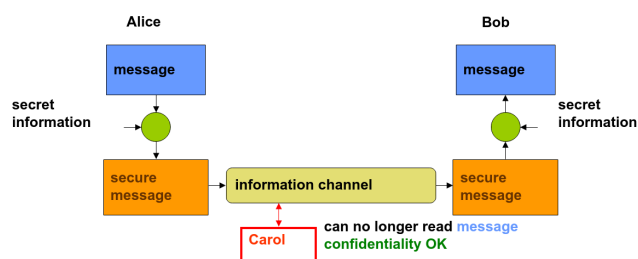
- Which security goals does this protocol fulfill?
- Which security goals per chapter?

#### 2.2.1 Confidentiality

- Data can only be read by those who are allowed to read the data
- Applications:
  - Communicating confidential data between branches of a corporation
  - Passwords
  - Storage of health data



(a) Passive attack by Carol: **eavesdropping** upon information channel



(b) Solution to eavesdropping

## Traffic-flow confidentiality

- Keeping secret who's communicating with whom
- Much harder to achieve than data confidentiality
- In Figure 2.1b data confidentiality is OK, traffic-flow confidentiality is NOT OK: Carol can still see that Alice is communicating with Bob

## Confidentiality vs Privacy

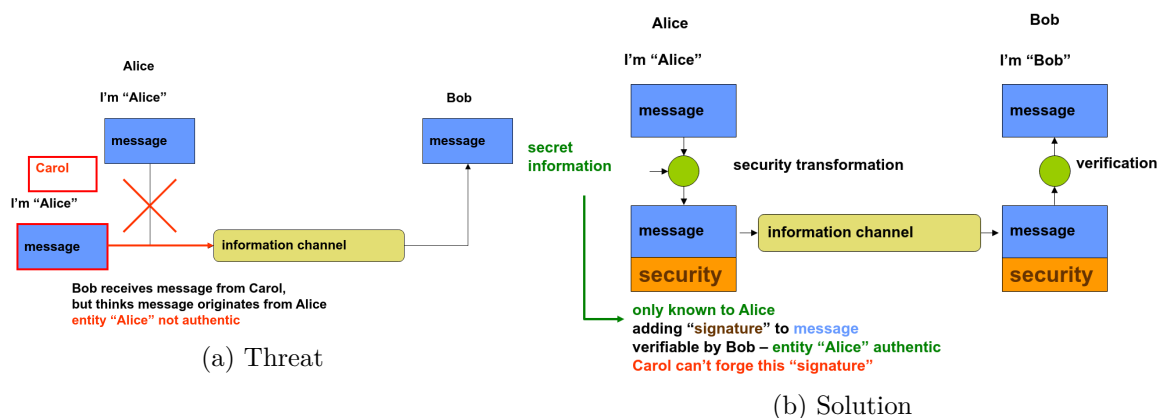
Privacy is having the right to choose what information you give away. It is a fundamental right, legally protected since long. Not every confidentiality requirement involves privacy: intellectual property in a business requires confidentiality, no privacy.

### 2.2.2 Authentication

Authentication is related to **identification**: it is the *electronic world* equivalent. *Is the person at the other end of the communication who he claims he is?*

Guaranteeing the authenticity of a communication is based on:

- **Entity** authentication: distinguish each entity from another based on collection of data. Each entity has a unique identity.
- **Attribute** authentication. Attribute = characteristic of an entity. Entities are often authenticated through authentication of some of its attributes. Do the communicating parties exhibit the characteristics they claim to have?
- **Data-origin** authentication: does the data indeed originate from the specified source? Important to evaluate whether data is reliable (**Data Integrity** see 2.2.4). Different from entity authentication: **no interaction with data source**.



### 2.2.3 Access Control/authorization

- Determines which user may access which resource (data, computation time, etc.)
- Requires **authentication of the entity** requesting access to these resources
  - System determines to what extent entity may access those resources
  - Access rights may **depend on entity itself or its attributes**

### Illustration 1: access control in OS

- Authentication through login and password
- Access control determined for this user (entity)
  - Full access to own files
  - Limited access to some other files
  - No access to other files
- Access rights different from user to user

### Illustration 2: access control to medical database

- Different rights for different types of Users
- Requires authentication based on specific **attributes**
- Access rights depend on attributes of the user
- Access rights different from user type to user type (**roles**)

## 2.2.4 Data integrity

- Guarantee that sent data and received data are identical
  - No tampering with data en route
  - Nothing was added
  - Nothing was deleted
  - Nothing was modified
  - Nothing was replayed
- stronger requirement than data origin authentication: data originates from specified source **AND** isn't changed on the way
- Threats
  - Messages can be replayed
  - Messages can be altered
  - Cannot be solved with confidentiality (encryption): encrypted messages can also be re-played

### Solution

A security footer containing a sequence number which can only be generated by the sender. This footer has to be generated based on the whole message to prevent tampering to the message itself. No need to encrypt the whole message for data integrity, but the message is not confidential if it isn't encrypted.

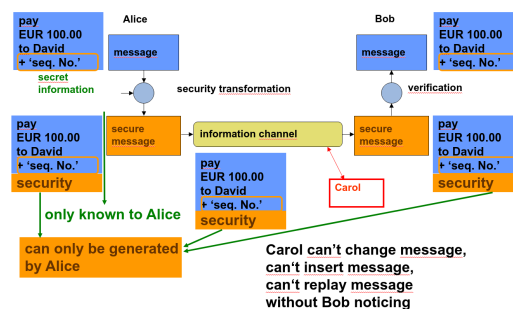


Figure 2.3: Data integrity solution

### 2.2.5 Non-repudiation

- Sender can't deny having sent the message. Important for receiver. *Prove order has been placed*
- Receiver can't deny having received the message. Important for sender. *Prove invoice has been paid*
- Both sides need to communicate and 'sign' their messages to guarantee non-repudiation for both sides.

### 2.2.6 Availability

- System/service is accessible and usable for authorised Users
- Security context  $\leftrightarrow$  System design context

### Threats

- DoS: denial-of-service: target swamped by torrent of messages from attacker
- DDoS: distributed denial-of-service: target swamped by torrent of messages from multiple (and numerous) senders (botnets).

## 2.3 Security Threats

Possible exam questions:

- **Explain the difference between confidentiality, authentication, access control/authorization, data integrity, non-repudiation and availability.**
- **Which of the above security goals are realized in the network protocols from Chapter 4?**
- **Why are sequence numbers (or nonces) added to messages? Is it a good idea to use a time stamp for this purpose?**
- **Which counter measurements can be taken against DoS and DDoS attacks?**
- **Give 5 examples of active attacks that can be used to compromise the security of a network protocol.**
- **Passive attacks**
  - Eavesdropping
  - Traffic analysis
- **Active attacks**
  - Message insertion/modification
  - Impersonation/masquerade
  - Replay
  - DoS
  - Hijacking (taking over existing connection, where attacker replaces sender or receiver)

Hackers first seek a weak point in a network (for example through social engineering), second they will use passive attacks to gain more information. Lastly they'll use active attacks.



### 2.3.1 Possible attacks

- Brute force: Trying all possible keys
- Cryptanalysis: using knowledge about structure of algorithm, pairs of plaintext and secure messages in order to recover plaintext message or key itself, or to forge secure message
- Side-channel attacks use physical properties or fault injection in order to recover plaintext or key
  - *Here's How iPhone Thermal Cameras Can Be Used to Steal Your Pin Codes* [6]
  - *Researchers crack the world's toughest encryption by listening to the tiny sounds made by your computer's CPU - ExtremeTech* [7]

### 2.3.2 Categories of attacks

- **Ciphertext only:** only secure message is known to attacker. Hardest one to break.
- **Known plaintext:** one or more pairs obtained with a single key are known to attacker. Easier to break, but still safe.
- **Chosen plaintext:** one or more pairs obtained with a single key, plaintext chosen by attacker. Harder to get, easier to break.
- **Chosen ciphertext:** one or more pairs obtained with a single key, ciphertext chosen by attacker (plaintext can be garbage). Even harder to get, easier to break.
- **Chosen text:** combination of chosen plaintext and chosen ciphertext.

### 2.3.3 Desired degree of security?

- Unconditionally secure is **not achieved by any practical security mechanism**.
- Computationally secure means that the **time required for breaking is longer than the usefull lifetime** of the information, or that the **cost of breaking the encryption is larger than the value** of the information.

# BIBLIOGRAPHY

- [1] S. Rodriguez, *1 in 10 in a survey think HTML is an STD* - *Los Angeles Times*, Mar. 2014. [Online]. Available: <https://www.latimes.com/business/technology/la-fi-tn-1-10-americans-html-std-study-finds-20140304-story.html> (visited on 09/24/2020).
- [2] M. Eeckhaut and Vanhecke Nikolas, *NSA hackt Belgische cyberprof* - *De Standaard*, 2014. [Online]. Available: [https://www.standaard.be/cnt/dmf20140131\\_049](https://www.standaard.be/cnt/dmf20140131_049) (visited on 09/24/2020).
- [3] S. Derix, G. Greenwald, and H. Modderkolk, *AIVD hackt internetfora, 'tegen wet in'* - *NRC*, 2013. [Online]. Available: <https://www.nrc.nl/nieuws/2013/11/30/aivd-hackt-internetfora-tegen-wet-in-a1429283> (visited on 09/24/2020).
- [4] F. Johannès and J. Follorou, *Révélation sur le Big Brother français*, Jul. 2013. [Online]. Available: [https://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais\\_3441973\\_3224.html](https://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html) (visited on 09/24/2020).
- [5] D. Ford, *Docs shielded Cheney defibrillator from hacks* - *CNN*, Oct. 2013. [Online]. Available: <https://edition.cnn.com/2013/10/20/us/dick-cheney-gupta-interview/index.html> (visited on 09/24/2020).
- [6] D. Cade, *Here's How iPhone Thermal Cameras Can Be Used to Steal Your Pin Codes*, Aug. 2014. [Online]. Available: <https://petapixel.com/2014/08/29/heres-iphone-thermal-cameras-can-used-steal-pin-codes/> (visited on 10/03/2020).
- [7] S. Anthony, *Researchers crack the world's toughest encryption by listening to the tiny sounds made by your computer's CPU* - *ExtremeTech*, Dec. 2013. [Online]. Available: <https://www.extremetech.com/extreme/173108-researchers-crack-the-worlds-toughest-encryption-by-listening-to-the-tiny-sounds-made-by-your-computers-cpu> (visited on 10/03/2020).